ROUTING AND TRANSMITTAL SLIP 1/28/85

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. D/COMMUNICATIONS		
2.		
3.		
4.		
5.		

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

#1 - FOR ACTION

(PLS PROVIDE DIRECT RESPONSE WITH A DROP CY TO EO/DDA.)

SUSPENSE: 15 FEBRUARY 1985

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

	Room No.—Bldg.
EO/DDA 7D18 HQS	Phone No.

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

* GPO: 1983 O - 381-529 (742)

DDA REGISTRY FILE 85-5

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS		X (For CH, SECOM)		
5	DDI				
6	DDA	X (For D/COMO)			
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO				
20					
21					
22					
	SUSPENSE		Date		

Remarks

STAT

STAT

STAT

3637 (10-81)

Date

DDA SUBJECT FILE COPY 0832

NTISSC
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC 6-/1
18 January 1985

MEMORANDUM TO THE MEMBERS OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

SUBJECT: Draft National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4000, "Guidelines for the Conduct of Communications Security (COMSEC) Monitoring Activities"

1. Enclosed is draft NTISSI No. 4000, subject as above. It replaces National COMSEC Instruction No. 4000A, same subject, dated 9 February 1984, and has been prepared in accordance with the provisions of National Security Decision Directive No. 145, National Policy on Telecommunications and Automated Information Systems Security, dated 17 September 1984.

2. Request you review the Enclosure and provide comments to the undersigned by 15 February 1985. My staff POC is [redacted] NSA (S081), 972-2509s/688-6130b. STAT STAT

3. Following receipt of comments, the draft NTISSI will be forwarded to the Attorney General. Upon Attorney General approval, the NTISSI will be issued by the National Manager.

STAT

[redacted]
Executive Secretary

Encl:
a/s

GUIDELINES FOR THE CONDUCT OF

COMMUNICATIONS SECURITY (COMSEC) MONITORING ACTIVITIES

NTISSI No. 4000
Date:

FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4000, Guidelines for the Conduct of COMSEC Monitoring Activities, establishes policy and guidelines for conducting COMSEC monitoring operations. It replaces National COMSEC Instruction No. 4000A, "Guidelines for the Conduct of COMSEC Monitoring Activities," dated 9 February 1984.

2. The heads of federal departments and agencies are responsible for developing procedures to implement NTISSI No. 4000 within their respective organizations. Additional copies of NTISSI No. 4000 may be obtained from the National Telecommunications and Information Systems Security Committee Executive Secretariat, National Security Agency, ATTN: S08.

LINCOLN D. FAURER
National Manager
for
Telecommunications and Automated
Information Systems Security

1. REFERENCES.

a. Communications Act of 1934, Public Law No. 73-416 (as amended).

b. Omnibus Crime Control and Safe Streets Act of 1968, Public Law No. 90-351 (as amended).

c. Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511.

d. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

e. National Security Decision Directive Number 145, "National Policy on Telecommunications and Automated Information Systems Security," dated 17 September 1984.

2. INTRODUCTION. The basic purpose of COMSEC monitoring is to provide unique material, not readily available through other sources, to evaluate the status of U.S. COMSEC. The information collected through the COMSEC monitoring program is similar to the information potentially available to foreign powers through their own signals intelligence (SIGINT) collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide a comprehensive data base for analysis. COMSEC monitoring is, therefore, used to provide the empirical data necessary to conduct comprehensive analyses of these vulnerabilities and afford a basis for correcting them.

3. PURPOSE AND SCOPE.

a. This Instruction provides policy and guidance for the establishment of COMSEC monitoring procedures consistent with law, Executive Orders, and applicable Presidential Directives.[1]

b. This Instruction is applicable to all federal government departments and agencies engaged in or using the results of COMSEC monitoring. It has been approved by the Attorney General.

[1]Although there are no federal statutes specifically addressing COMSEC monitoring, References a., b., and c. will have an impact upon any COMSEC monitoring guidelines and procedures.

c. Technical surveillance countermeasures, electronic sweeps, surveillance of noncommunications emissions (e.g., radar), and TEMPEST testing are not within the scope of this Instruction.

4. DEFINITIONS.

a. COMSEC. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to telecommunications systems generating, handling, processing, or using classified or sensitive but unclassified information. It also includes the application of physical security measures to COMSEC information or materials.

b. COMSEC Monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions.

c. Contents. When used with respect to a communication, it includes any information concerning the identity of the parties to such communication or the existence or meaning of that communication.

d. Electronic Surveillance. The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

e. Private Communication. A communication in which the parties thereto, in the absence of their consent to be monitored for COMSEC purposes, have a reasonable expectation of privacy.

f. Telecommunications. The preparation and transmission of information by electrical, electromagnetic, electromechanical, or electro-optical means.

g. Telecommunications System. The devices used to transmit and/or receive communications or process telecommunications, including the preparation of information, therefor; the devices may be electrical, electromagnetic, electromechanical, or electro-optical.

h. Government Telecommunications. Telecommunications of any employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a government contractor. (See Telecommunications and Telecommunications System, above.)

5. POLICY.

a. The government will conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to government telecommunications and aid in countering their vulnerability. Such activities shall be conducted in strict compliance with law, Executive Orders, applicable Presidential Directives, and this Instruction.

b. Government telecommunications systems are subject to COMSEC monitoring by duly authorized government entities. The use of such systems by any person shall be construed to imply consent to the monitoring for COMSEC purposes of communications carried over them.[2] Users of these systems must be properly notified in advance, in accordance with the guidelines in subparagraph 6.e., below, that their use of these systems constitutes consent to monitoring for COMSEC purposes. The government shall not monitor telecommunications systems which are owned or leased by government contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization (or his designee) and the written opinion of the general counsel of the department or agency which is conducting the monitoring that procedures, such as those contained in subparagraph 6.e., below, have been implemented sufficiently to afford adequate notice to the contractor organization's employees.

c. The government shall not monitor for COMSEC purposes the contents of any telecommunication when such monitoring would constitute electronic surveillance.

d. In accordance with procedures approved by the Attorney General, information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction. When taking such

[2] Consent to COMSEC monitoring is required of only one party to a conversation or transmission.

action, the general counsel of the department or agency which is conducting the COMSEC monitoring shall be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the general counsel of the department or agency which performed the monitoring.

e. The results of COMSEC monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Reference d. However, the results of COMSEC monitoring of U.S. and Allied military exercise communications may be used for exercise intelligence purposes under procedures prescribed in applicable directives.

f. No department or agency may monitor the telecommunications of another department or agency for COMSEC purposes without the express prior written approval of a responsible official of the department or agency to be monitored, except as provided for in subparagraph 8.b.(2).

g. It is recognized that COMSEC monitoring operations conducted in a crowded telecommunications environment may result in the temporary acquisition of private communications. COMSEC monitoring shall be conducted in accordance with operational procedures which minimize the possibility that the contents of such telecommunications will be acquired. Such procedures shall be consistent with the guidelines contained herein and shall be endorsed by the general counsel of the department or agency issuing the procedures.

6. GUIDELINES FOR THE CONDUCT OF COMSEC MONITORING.

a. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 2., above:

(1) To collect operational signals needed to measure the degree of security being achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

(2) To provide a basis from which to assess the types and value of information subject to loss through intercept and exploitation of government telecommunications.

(3) To provide an empirical basis for improving the security of government telecommunications against SIGINT exploitation.

(4) To assist in determining the effectiveness of Electronic Countermeasures/Electronic Counter-Countermeasures (ECM/ECCM) and cover and deception measures.

(5) To identify government telecommunication signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide SIGINT elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

(6) To provide empirical data to train users of government telecommunications systems in proper COMSEC techniques and measures.

(7) To evaluate the effectiveness of COMSEC education and training programs.

(8) To train personnel and to test the capability of COMSEC monitoring equipment.

b. The following categories of telecommunications are not considered private for purposes of this Instruction. Accordingly, acquisition of the contents of any communications in these categories which may occur in the course of locating or examining government telecommunications is not electronic surveillance.

(1) Radio or television broadcast communications, whether commercial, public, or educational, intended for the information or entertainment of the general public.

(2) Public safety, citizens band, amateur radio, and similar radio systems licensed by the government for public use or access.

(3) Any communications in portions of the electromagnetic spectrum which are allocated by the government for its own use.

c. No incidentally acquired private communication may be monitored beyond the point where a determination can reasonably be made that it is private. A record of the acquisition may be kept for signal identification and avoidance purposes; such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the contents of the communication.

d. Contents of any private communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a government communication.

e. Notice of the existence of COMSEC monitoring in conformance with subparagraph 5.b., above, can be accomplished by any of the following means or any combination thereof which the legal counsel of the affected department or agency considers legally sufficient to achieve proper notification in terms of content, prominence, and specificity.

(1) Decals placed on the transmitting or receiving devices.

(2) A notice in the daily bulletin or similar medium.

(3) A specific memorandum to users.

(4) A statement on the cover of the official telephone book or communications directory.

(5) A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

7. CONTROL OF MONITORING RECORDS AND EQUIPMENT.

a. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or material produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least CONFIDENTIAL and downgraded to UNCLASSIFIED when security weaknesses are corrected.

b. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes except as provided for in subparagraph 5.d., above. These reports shall not contain any information extraneous to COMSEC purposes or names of individuals or sufficient data to identify the source except in an official capacity; e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

c. All COMSEC monitoring recordings and written records, logs, and notes shall be destroyed as soon as operationally feasible.

d. Except as provided for in subparagraph 5.d., above, no information extraneous to COMSEC purposes will be recorded, reported, noted, logged, or filed. If within the capabilities of COMSEC monitoring equipment, any such information that is inadvertently acquired shall be expunged upon recognition. All

monitoring records shall be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

e. Access to and dissemination of COMSEC monitoring recordings or written records, reports, logs, and notes shall be limited to that which is necessary for COMSEC purposes. No access to, or dissemination of, such materials beyond COMSEC operational elements shall be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

f. COMSEC monitoring equipment shall be safeguarded to prevent unauthorized access and use.

8. RESPONSIBILITIES.

a. Heads of departments and agencies shall:

(1) Provide for and conduct COMSEC monitoring operations as they deem appropriate, subject to the provisions of law, Executive Orders, applicable Presidential Directives, and this Instruction.

(2) Develop procedures for the conduct of COMSEC monitoring, consistent with the policy and guidelines herein, in collaboration with the Director, NSA. Such procedures shall be approved by the Attorney General.

(3) Notify, as specified in subparagraph 6.e., all personnel and contractors who are present on facilities of the department or agency of the policy in subparagraph 5.b., above.

(4) Certify annually to the Attorney General that all personnel and contractors have been informed of the provisions of this Instruction and any individual procedures developed in accordance with subparagraph 8.a.(2), above.

b. The Director, NSA, shall:

(1) Advise and assist other departments and agencies in establishing their operating procedures to implement this Instruction.

(2) Conduct COMSEC monitoring of government telecommunications as necessary to discharge his responsibilities under National Security Decision Directive Number 145, provided that no monitoring shall be performed without first providing timely notification of such monitoring to the heads of the departments or agencies to be monitored.

c. The Attorney General shall report annually to the Director, NSA those departments and agencies which have forwarded certification required by subparagraph 8.a.(3), above.

DISTRIBUTION:

NSA SPECIAL DISTRIBUTION
NSC
ASD(C^3I) (2)
DUSD(P) (ATTN: DIR CI&SP
and DIR C^2 POLICY) (2)
OJCS (C^3I) (2)
CSA (DAMI-CIC) (5)
CNO (3)
CMC (CCT) (5)
CSAF (XOK) (5)
HQ SPACECOM (KR) (2)
CINCLANT (J6) (2)
CINCMAC (DC) (2)
CINCPAC (C^3S) (2)
CINCSAC (DC) (2)
USCINCEUR (C^3S) (2)
USCINCRED (RCC4S) (2)
USCINCSO (J6) (2)
USCINCCENT (CCJ6) (2)
COMUSFCARIB (J6) (2)
COMUSJAPAN (J6) (2)
COMUSKOREA (J6) (2)
DIR TRI-TAC (TT-SC) (2)
DIR TRI-TAC JTE (TT/TE-C)
CDR USAINSCOM,
(IAOPS-OP-P) (15)
COMNAVSECGRU (G-61) (15)
COMNAVTELCOM (Code 1243) (5)
DCMS (T30) (3)
CGMCDEC (DEVCEN C^3) (2)
AFCSC (EPPP)
DCA (Code B315) (20)
DIA (RCM-4)
DIS (VO410) (5)
DLA (DLA-TI) (2)
DNA (LECD) (2)
Dept. of Agriculture
(MSD/FAS) (2)
Dept. of Commerce (I&S) (2)
Dept. of Energy (CSTM) (2)

Dept. of Health & Human Svcs (IG) (2)
Dept. of Interior (AMO) (2)
Dept. of Justice (SPS JMD) (2)
Dept. of State (ASC) (2)
Dept. of Transportation (Security Staff, M-441) (2)
Dept. of Treasury (ADTM) (10)
CIA (OC-CSD) (2)
FAA (ACS300) (2)
FCC (Code 22800) (2)
FBI (TSD) (2)
FEMA (RMIR-IM-TW-CS) (7)
GSA (Code KJS) (2)
NASA (NIS-5) (2)
NCS (AO) (2)
NRC (DS 286-SS) (2)